

Operator's Lesson Plan

I. IDACS Coordinator Duties and Responsibilities

A. The agency head appoints the IDACS Coordinator by notifying IDACS in writing.

B. The following are terminal coordinator responsibilities as listed in the Indiana Administrative Code (IAC).

240 IAC 5-2-8 Terminal agency operations; coordinator; duties and responsibilities.

Authority: IC 10-1-1-3; IC 10-1-2.5-7

Affected: IC 10-4-1-6-7; IC 10-1-2.5-3

Sec. 8. Once operational on the IDACS System, each terminal agency is required to designate one (1) individual as coordinator to serve as liaison between that department and the IDACS committee. It is important that the person selected becomes familiar with all phases of IDACS to efficiently carry out all duties and responsibilities assigned.

Duties and responsibilities are as follows:

1. All agency personnel, including any non-terminal agencies serviced, utilizing system information are aware of the rules and policies of the IDACS/NCIC/NLETS system.
2. Disseminate the contents of the IDACS/NCIC newsletters to all terminal operators and non-terminal agencies serviced.
 - a. The intent of the newsletter is to keep users informed.
3. Validation reports are properly processed.
4. Terminal operators receive proper IDACS training in accordance with the IDACS certification-training program.
5. Inform IDACS of any changes in the agency head, coordinator, agency address, or terminal site.
6. Report all IDACS rules violations and other improper uses to IDACS.

II. System Officials and Organization

A. The following are IDACS Committee Rules as listed in the Indiana Administrative Code (IAC).

240 IAC 5-1-1 General policy: restrictions on use

Authority: IC 10-1-1-3; IC10-1-2.5-7

Affected: IC 10-1-2.5-2

Operator's Lesson Plan

Sec. 1. (a) A committee appointed by the Superintendent of the Indiana State Police, for the purpose of managing and controlling the Indiana Data and Communications System hereinafter called "IDACS", has the responsibility for the management of the statewide system network as imposed by these rules and as directed by the Superintendent of the State Police. The committee chairman shall be selected by the Superintendent. The chairman shall report activities of the committee to the Superintendent for review and approval. To make sure the proper operation of the systems, the standards, procedures, formats, and criteria as set forth herein shall be strictly adhered to. In this respect, as in system security, the IDACS terminal agency shall not only follow the rules set forth, but shall also ensure that agencies they are servicing do the same.

B. IDACS Committee Membership

1. The IDACS Committee is composed of several voting members, a chairman, and a number of non-voting members appointed by the State Police Superintendent.
2. Voting members of the committee are as follows:
 - a. Chairman (votes only in a tie situation)
 - b. Indiana Sheriff's Association
 - c. Indiana Chiefs of Police Association
 - d. State Police Records Division
 - e. State Police Communications Division
 - f. State Police Criminal Justice Data Division
 - g. State Police IDACS Section
 - h. State Police Systems & Programming
 - i. IDACS Area I Representative
 - j. IDACS Area II Representative
 - k. IDACS Area III Representative
 - l. IDACS Area IV Representative
 - m. IDACS Area V Representative
3. Non-Voting members of the committee:
 - a. IDACS Security Officers
 - b. Data Operations Section
 - c. Fiscal Division
 - d. Legal Advisor

Operator's Lesson Plan

4. IDACS Committee meetings are held once every quarter normally on the first Tuesday of the following months: March, June, September, and December.
 - a. The meeting is open to all interested persons.
5. Area Representatives
 - a. Area Representatives will be nominated every two (2) years by the Area they are to represent.
 - b. Nominees shall be either the IDACS Coordinator or in a management position for an IDACS Terminal Agency.
 - c. The nominee must be approved by the State Police Superintendent.
 - d. Represents his/her Area on the IDACS Committee.
 - e. Area Meetings
 1. Must have at least one (1) Area meeting during each half of the calendar year.
 2. The meeting is opened to all IDACS Coordinator's in the Area.
 3. The meeting is designed to inform Area Representatives of the IDACS Coordinator's concerns and suggestions for input to the IDACS Committee. It is also designed for Area Representatives to inform IDACS Coordinator's of the work being conducted by IDACS.

III. Terminal Agency User Agreements and Security

- A. The following is information concerning terminal agency user agreements and system security as listed in the Indiana Administrative Code (IAC).

240 IAC 5-2-9 User Agreement

Authority: IC 10-1-1-3; IC 10-1-2.5-7

Affected: IC 5-2-5; IC 10-1-2.5-4

Sec. 9. (a) All IDACS user agencies shall complete a "user agreement" before utilizing the system. Agencies with terminals and statutory police agencies shall complete such agreements with the Indiana State Police and the IDACS Committee. Non-terminal agencies shall complete an agreement with the terminal agency that services them. Agencies that only have mobile data devices (MDD's) and that have direct access to IDACS/NCIC, must sign a terminal agency user agreement with the Indiana State Police.

- B. Purpose of Agreement

1. This agreement provides for the IDACS Committee to serve as the agency responsible for the exchange of statewide criminal offender

Operator's Lesson Plan

record information and other criminal justice and law enforcement information between IDACS and the terminal agency. In addition, it provides for the Indiana State Police to serve as the State Control Terminal agency to facilitate the interchange of wanted file/computerized criminal history record information between NCIC and the terminal agency and message switching functions between NLETS and the terminal agency, via the IDACS network.

C. Terminal/Non-Terminal Agency Agreements

1. This agreement provides for the IDACS terminal agency to serve as the agency responsible for the exchange of statewide criminal offender record information and other criminal justice and law enforcement information between IDACS and the non-terminal agency. In addition, it provides for the terminal agency to serve as the agency to facilitate the interchange of wanted file/computerized criminal history record information between NCIC and the non-terminal agency and message switching functions between NLETS and the non-terminal agency, via the IDACS network.
2. Those agencies that only have mobile data devices (MDD's) must sign a non-terminal agency user agreement with the terminal agency that services them (i.e. entries, validations, CHRI, III, etc.).
3. Each terminal agency must keep on file copies of the Terminal Agency User Agreement and any terminal/non-terminal agency agreements with the agencies they service. These agreements must be made available upon request of the IDACS Security Officer.
4. New agreements are required when the agency head changes.

D. Who May Access System Data

240 IACa 5-2-10 Security; confidentiality

Authority: IC 10-1-1-3; IC 10-1-2.5-7

Affected: IC 10-1-2.5

Sec. 10. (a) "SYSTEM" as used in the security and confidentiality rules means IDACS, NLETS, and/or NCIC terminals, equipment and any and all data accessible from or stored therein.

1. Access, meaning the ability to obtain from the System, shall be permitted only to criminal justice agencies in the discharge of their official

Operator's Lesson Plan

mandated responsibilities, and those agencies as required by state and/or federal enabling authority. Agencies that shall be permitted access to SYSTEM data include the following:

- a. Police forces and departments at all governmental levels (including private college and railroad police departments as authorized by Indiana Code) that are responsible for enforcement of general criminal laws.
- b. Prosecutive agencies and departments at all governmental levels.
- c. Courts at all governmental levels with a criminal or equivalent jurisdiction.
- d. Correction departments at all governmental levels, including corrective institutions and probation departments.
- e. Parole commissions and agencies at all governmental levels.
- f. Agencies at all governmental levels which have as a principle function the collection and provision of fingerprint identification information.
- g. Regional or local governmental organizations established pursuant to statute which collect and process criminal justice information and whose policy and governing boards have, as a minimum, a majority composition of members representing criminal justice agencies.
- h. Approved noncriminal justice agencies may have access to SYSTEM data on a limited basis. "Limited basis" means restricted to only that data recommended through resolution by the IDACS committee and approved by the State Police Superintendent.

E. Terminal Security Measures

1. All agencies and computer centers having devices on the SYSTEM and/or having access to SYSTEM data shall physically place these devices in a secure location previously approved by the IDACS Committee within the authorized agency. Subsequent physical location changes of devices shall have prior approval of the IDACS Committee.

Operator's Lesson Plan

- a. A secure location is defined as: secure from public access and view of the screen and/or printed data.

F. Personnel Security Measures (Device Operators)

1. Since personnel at these computer centers have access to data stored in the SYSTEM, they shall be screened thoroughly under the authority and supervision of the IDACS committee or their designated representative.
2. This screening shall also apply to noncriminal justice maintenance or technical personnel. The screening process shall consist of a character investigations, including fingerprints, for the purpose of establishing suitability for the position. Investigations shall consist of the gathering of information as the applicant's honesty, integrity and general reputation. Personal characteristics or habits, such as lack of judgment, lack of physical or mental vigor, inability to cooperate with others, intemperance, or other characteristics which would tend to cause the applicant to be unsuitable for this type of position, shall be considered sufficient grounds for rejection. Convincing information in an applicant's past history involving moral turpitude, disrespect for law, or unethical dealings shall be considered sufficient grounds for rejection. If any of the above facts are presented to the IDACS committee, a recommendation shall be made and presented to the State Police Superintendent for a final approval or disapproval decision.

G. System Data Security

1. Audit requirements of SYSTEM data.

240 IAC 5-1-2 Audit of system transactions

Authority: IC 10-1-1-3; IC 10-1-2.5-7

Affected: IC 10-1-2.5-3

Sec. 2. (a) Established IDACS committee policy requires all user agencies to Maintain an audit trail for six (6) months for certain types of IDACS transactions as itemized but not limited to the following:

1. Administrative Messages (AM) (both transmitted and received).
2. Bureau of motor vehicles and department of natural resources information file data.
3. IDACS/NCIC stolen file data.

Operator's Lesson Plan

4. Out-of-State (NELTS) Bureau of Motor Vehicles or Department of Natural Resources data.
 - a. These audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated. Audit trails shall be maintained manually or by automation, and shall be made available to the IDACS Committee for inspection upon request.
 - b. It should be noted that these are minimum requirements and it may be necessary to keep important or case related information for longer periods of time in order to properly confirm or validate IDACS/NCIC wanted entries.
5. Audit requirements for Criminal History Data
 - a. NCIC and IDACS require that an audit trail for the dissemination of criminal history be kept for one (1) year. This includes the Violent Gang and Terrorists Organization File (VGTOF) and Sexual Offender File (SOF).

240 IAC 5-1-3 Audit of Criminal History Record Dissemination

Authority: IC 10-1-1-3; IC 10-1-2.5-7

Affected: IC 4-1-6; IC 10-1-2.5-3

Sec. 3. 28 U.S.C. states that audits shall be kept pertaining to the dissemination of criminal history records. This includes responses from NCIC's Interstate Identification Index (NCIC III) and responses from state central repositories and other agency criminal history files (both in-state and out-of-state). Such audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated.

- b. The Violent Gang and Terrorists Organization File is in NCIC only. The information in the VGTOF file is provided in the "Hot" file format. NCIC's and IDACS policy is to treat the VGTOF file as Criminal History.
3. IDACS/NCIC Wanted/Stolen File Entry/Audit
 - a. All entries into the IDACS/NCIC Wanted/Stolen files shall be supported by written documentation in the form of a warrant,

Operator's Lesson Plan

or a case/incident report filed by the investigating officer. This documentation shall be maintained and available at all times, for as long as the entry remains in file.

4. Entry Requirements for SYSTEM Data.

Authority: IC 5-2-5-12(a) effective 7-1-1998

Sec. 12. (a) On a daily basis, all law enforcement agencies shall enter into the Indiana Data and Communications System (IDACS) computer the following:

1. All information concerning stolen or recovered property including:
 - a. Motor vehicles
 - b. Firearms
 - c. Securities
 - d. Boats
 - e. License Plates
 - f. Other Stolen or recovered property
 2. All information concerning fugitives charged with a crime, including information concerning extradition.
 3. All information concerning runaways, missing as well as unidentified persons, and missing children (as defined in IC 10-1-7-2), including information concerning the release of such persons to the custody of a parent or guardian.
 4. Information contained in a protective order, including any modifications or extensions issued by a court and filed with a law enforcement agency as required in IC 5-2-9-6(f).
- (b) On a daily basis, all law enforcement agencies shall:
1. All information concerning missing children (as defined in IC 10-1-7-2) in the National Crime Information Center's (NCIC) Missing Person File.
 2. Enter into the National Crime Information Center's (NCIC) Wanted Person's File all information concerning warrants for a person who allegedly abducted or unlawfully retained a missing child.
 3. All information concerning an unidentified person into the National Crime Information Center's (NCIC) Unidentified Person File.

Operator's Lesson Plan

- a. If a protection order is removed from the depository established under IC 5-2-9, the law enforcement agency responsible for the depository shall delete the information entered under subsection (a) (4) from the Indiana Data and Communications System (IDACS) computer.
- H. IDACS is primarily a system for law enforcement/criminal justice users and as such only data related to law enforcement/criminal justice shall be transacted by the system. Information furnished through the system shall be restricted to the use of authorized law enforcement/criminal justice agencies, or those authorized noncriminal justice agencies performing criminal justice responsibilities, and shall not be sold, transmitted, or disseminated to any noncriminal justice agency or person unless authorized by the State Police Superintendent. Such authorization for dissemination can occur when it has been determined that to do so would be in the best interest of the law enforcement/criminal justice community.
 - 1. Exceptions:
 - a. Road and weather data, which can be released to the public.
 - b. Hazardous materials data can be given to fire departments, state board of health, and health care providers in emergency situations.
 - 2. Missing person data in accordance with the 1982 Missing Children's Act, which the IDACS Committee adopted on 10-02-1984. The Act stipulates that the user agencies can confirm entries on Unemancipated juveniles to parents, legal guardians and next of kin.

IV. Validation Procedures

240IAC 5-2-7 Validation of Records

Authority: IC 10-1-1-3; IC 10-1-2.5-7

Affected: IC 4-1-6-7; IC 10-1-2.5

Sec. 7. (a) All IDACS user agencies shall validate, on a periodic basis, as prescribed to the user agency by IDACS, all IDACS wanted records entered on their authority. Validation of records shall be in conformity and compliance with rules set forth by IDACS.

- (b) Validation obligates the originating agency to confirm the record is COMPLETE, ACCURATE and is still OUTSTANDING or ACTIVE.

Operator's Lesson Plan

- (c) Validation is accomplished by reviewing the original entry and current supporting documents and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. In the event the originating agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority shall make a determination based on the best information and knowledge available whether or not to retain the original entry on file.
- (f) To ensure the validity of IDACS and NCIC records, administrative controls shall be maintained which will result in the prompt updating for the benefit of system users. Agencies entering records in IDACS and/or NCIC are solely responsible for their accuracy, timeliness, and completeness. Only by conscientious validation of records can users remain assured the integrity of the system is being upheld, and inquiring officers can rely on the information in IDACS and NCIC.
- (g) The Indiana Control Terminal (Indiana State Police) is responsible to the national network (NCIC). Control terminal responsibilities are as follows:
 - 1. Monitor system use.
 - 2. Enforce discipline.
 - 3. Assure that all users meet policy and system procedures.
 - 4. Maintain validation schedule as established by NCIC/IDACS.
- (h) Procedures for documentation are as follows:
 - 1. Each agency shall receive an automated validation notice in compliance with the validation schedule.
 - 2. It shall be the responsibility of the originating agency IDACS coordinator to cause each record to be processed according [sic.] to subsection (c) and to ensure that any errors are corrected, inactive records are removed, and active records are kept in the system by submitting the appropriate validation transaction.
 - 3. An agency that allows IDACS to purge inactive or unwanted records from the wanted files shall be subject to sanction.

Operator's Lesson Plan

B. Validation Schedule

Validation	Entries Made On
January	October
February	November
March	December
April	January
May	February
June	March
July	April
August	May
September	June
October	July
November	August
December	September

C. Validation Process

1. On or about the twentieth (20th) of the current month the Open Fox Switch will generate an initial notification transaction to each ORI that has records in the system requiring validation.
2. This notification will contain records that were entered based on the **date of entry** not on the date of theft.

Validation Initial Notification:

THIS MESSAGE SUMMARIZES THE SEPTEMBER RECORDS
REQUIRING VALIDATIONS BY YOUR AGENCY WITHIN 40 DAYS OF
THIS NOTICE.

STOLEN GUN	1
STOLEN LICENSE PLATE	3
STOLEN VEHICLE	3
TOTAL	7

3. Each ORI that does not complete their validations will receive an additional notification 20 days and 10 day's before validations are due.

Operator's Lesson Plan

Example:

Validation Initial Notification:

20 DAYS HAVE PASSED SINCE THE INITIAL SEPTEMBER VALIDATION NOTIFICATION. THE FOLLOWING IS A SUMMARY OF THE SEPTEMBER RECORDS PENDING VALIDATIONS BY YOUR AGENCY. THE RECORDS WILL BE PURGED IF NOT VALIDATED ON TIME.

STOLEN GUN	1
STOLEN LICENSE PLATE	3
STOLEN VEHICLE	3
TOTAL	7

4. No record can be validated after midnight of the last day of the month the record is due to be validated.
5. Terminal agencies are responsible for the on-line validation processing of returned records for non-terminal agencies they support.

Operator's Lesson Plan

D. Local Agency Validation Procedures

1. Query Validation System (QVAL)

- a. The QVAL transaction is utilized to obtain a summary of the records that require validation by an ORI. This screen can be used at anytime so that the agency validating the records will not have to wait for an unsolicited message from Open Fox.

The screenshot shows the Omnibox Force application window. The title bar reads "Omnibox Force". The menu bar includes "File", "Forms", "Edit", "Comm", "Options", "Tools", "Windows", "Links", and "Help". The toolbar contains icons for "Transmit", "Message Window", and "Message Log". The main window is titled "QUERY VALIDATION SYSTEM (QVAL)". It contains two sections: "USER DATA" and "AGENCY/CASE DATA".

USER DATA

- User ID (UID): TTESTER
- Password Field (PWID):
- Entering Agency (ENT):
- Requestor (RQR):

AGENCY/CASE DATA

- Originating Agency Code (ORI): INISP0000
- Optional Control Field:

At the bottom of the window, there is a "Command:" field and a status bar. The status bar displays "FOX-PRIM", "T", "SPHQ00X8", "TTESTER", "LOG", "0 Message", and "10:27". The Datamaxx logo is in the bottom left corner, and "Leading Law Enforcement Technology" is in the bottom right corner.

- b. Example of response:

Date/Time

20040223111958

Ent Agy

Summary

QVAL: TESTER, IDX, TEST RECORDS, INISP00T1

TXT

Operator's Lesson Plan

THE FOLLOWING IS A SUMMARY OF FEBRUARY RECORDS
REQUIRING VALIDATION

BY YOUR AGENCY:

STOLEN LICENSE PLATE 1

TOTAL 1

*** END OF RESPONSE ***

MRI 599926 IN: MFOX 386 AT 23FEB2004 11:19:58

OUT: SPHQ00X9 2 AT 23FEB2004 11:19:58

2. Query Validation System Records (QVAD)
 - a. The QVAD transaction is utilized to specify the type and number of records to be returned for validation processing.

The screenshot displays the Omnibox Force application window. The title bar reads "Omnibox Force". The menu bar includes "File", "Forms", "Edit", "Comm", "Options", "Tools", "Windows", "Links", and "Help". The toolbar contains icons for "Transmit", "Message Window", and "Message Log". The main window is titled "QUERY VALIDATION SYSTEM RECORDS (QVAD)". It contains three sections: "USER DATA" with fields for "User ID (UID)" (containing "TTESTER"), "Password Field (PWD)", "Entering Agency (ENT)", and "Requestor (RQR)"; "AGENCY/CASE DATA" with fields for "Originating Agency Code (ORI)" (containing "INISP0000") and "Optional Control Field"; and "RECORD DATA" with fields for "Beginning Message Number (BMN)", "Ending Message Number (EMN)", "Validation File Type (FIL)", and "Validation File Month (MON)". At the bottom, there is a "Command:" field and a status bar showing "FOX-PRIM", "T", "SPHQ00X8", "TTESTER", "LOG", "0 Message", and "10:28". The Datamaxx logo and "Leading Law Enforcement Technology" are visible in the bottom right corner.

- b. Record Data

Operator's Lesson Plan

1. Beginning Message Number (BMN)
 - a. Required.
 - b. 0001, etc.

2. Ending Message Number (EMN)
 - a. Required.
 - b. 0005, etc.
 - c. A maximum number of 20 records can be requested. Requesting more than 20 records may cause the system to become incapacitated.

3. Validation File Type (FIL)
 - a. Required.
 - b. C-Convicted Person, Z-Gang/Terrorist Group, T-Gang/Terrorist Group, G -Lost, Stolen & Recovered Guns, M- Missing Persons, H-Protection Order Person, X-Sexual Offender Person, B-Stolen Boat, P-Stolen License Plates, S-Stolen Securities, V-Stolen Vehicles, Vehicle/Boat Part, U-Unidentified Person, W- Wanted Persons.

4. Validation File Month (MON)
 - a. 01 (January) through 12 (December)

3. The response will return the specified records that have not been validated.

Example:

Summary

QVAD: TESTER, IDX, TEST RECORDS, INISP00X9

TXT

**\$C

MKE/I_EW

ORI/INISP00X9

NAM/SMITH,OTIS

SEX/M

RAC/W

DOB/19500101

HGT/509

WGT/280

EYE/BRO

HAI/BRO

OFF/4290

DOW/20040308

Operator's Lesson Plan

OLN/1111111111
 OLS/IN
 OLY/2005
 OCA/2004-03-1
 MIS/TEST RECORD
 DTE/20040308
 IDX/WX00155062
 OLN/1234566789 OLS/NC OLY/2006
 **
 **\$C

MKE/EW
 ORI/INISP00X9
 NAM/MAN,BAD
 SEX/M
 RAC/W
 DOB/19800710
 HGT/509
 WGT/200
 EYE/BRO
 HAI/BRO
 OFF/5310
 DOW/20040319
 OCA/2004-03-1
 MIS/TEST RECORD
 NIC/W735672584
 DTE/20040319
 IDX/WX00161338

**

*** END OF RESPONSE ***

MRI 6317564 IN: MFOX 363 AT 01JUN2004 13:04:08
 OUT: SPHQ00X9 3 AT 01JUN2004 13:04:08

4. Upon receipt of the notification, agencies should begin their local validation procedures in accordance with 240 IAC 5-2-7.
5. Agencies should make any additions, corrections, or deletions necessary to each record based on a review of the supporting documents. Each record must be validated with the appropriate transaction in order for the record to remain in file.
6. Non-Terminal Agencies should contact the terminal agency that handles IDACS transactions for them to make the necessary additions, corrections, deletions, or validations.

Operator's Lesson Plan

7. Regardless of whether or not your agency has a terminal, it is imperative that you take action on each record listed on the report. **Unwanted records are not to be left in file for the automated purge process. These records are to be removed from file by the entering agency.**
8. It is imperative that these procedures are followed. Failure to properly validate could jeopardize officer safety. It will also place you and your agency in a liability situation. Agencies who fail to abide by these rules are subject to sanction.
9. Validation procedures must be formalized and copies of these procedures must be on file for review during an IDACS or NCIC audit.

E. Validation Transactions

1. Each record that is to remain in file must have a validation transaction submitted. This transaction will update the VLN Field in each record with the person responsible for checking the record.
2. To validate multiple records, select the Validate Multiple Records (VALM) screen. This form can be used to validate records from one (1) to ten (10).
 - a. If all records being validated are from the same case, the master OCA Field must contain "Y" – Yes in the Identifying Data Record 1. The OCA will not have to be entered in the Identifying Data Record 2 through 10.
 - b. If all records being validated are of the same file, the Message Key (MKE) field must contain "Y" – Yes in the Identifying Data Record 1. The MKE field will not have to be filled out in Identifying Data Record 2 through 10.
 - c. Ten different cases can be validated. The Master OCA field must contain "N" – No.
 - d. Ten different records can be validated. The Message Key (MKE) field must contain "N" – No.
 - e. The command bar function for Validate Multiple Records: TF VALM.

Operator's Lesson Plan

Omnibx Force

File Forms Edit Comm Options Tools Windows Links Help

Transmit Message Window Message Log

VALIDATE MULTIPLE RECORDS (VALM)

AGENCY/CASE DATA

Originating Agency Code (ORI)

Name of Validator (VLN)

IDENTIFYING DATA - RECORD 1

IDX Number (IDX) NIC Number (NIC)

Agency Case Number (OCA) Message Key (MKE)

Master OCA Master MKE

IDENTIFYING DATA - RECORD 2

IDX Number (IDX) NIC Number (NIC)

Agency Case Number (OCA) Message Key (MKE)

IDENTIFYING DATA - RECORD 3

IDX Number (IDX) NIC Number (NIC)

Agency Case Number (OCA) Message Key (MKE)

IDENTIFYING DATA - RECORD 4

IDX Number (IDX) NIC Number (NIC)

Agency Case Number (OCA) Message Key (MKE)

IDENTIFYING DATA - RECORD 5

IDX Number (IDX) NIC Number (NIC)

Agency Case Number (OCA) Message Key (MKE)

Command:

FOX-PRIM T SPHQ00X8 VNOWACZE... LOG 0 Message 16:03

Datamaxx Leading Law Enforcement Technology

- a. Identifying Data – Record 1
 1. IDX Number (IDX)
 - a. Enter IDX Number.
 2. NIC Number (NIC)
 - a. Enter NCIC Number.
 3. Agency Case Number (OCA)
 - a. Minimum of one and a maximum of twenty alphanumeric characters.
 4. Message Key (MKE)
 - a. Enter valid message key.
 5. Master OCA
 - a. Y – Yes.
 - b. N – No.

Operator's Lesson Plan

6. Master Message Key (MKE)
 - a. Y – Yes.
 - b. N – No.
3. To validate a record with modifications, select the modify screen for the record type. Example: If a stolen gun is to be validated with a modification, go to the Forms Menu, under guns, select Modify Gun (MG) or TF MG on the Command Bar of the Omnixx Force Screen.

Omnixx Force

File Forms Edit Comm Options Tools Windows Links Help

Transmit Message Window Message Log

MODIFY STOLEN GUN TRANSACTION (MG)

USER DATA

User ID (UID)

Password Field (PWD)

Entering Agency (ENT)

Requestor (RQR)

AGENCY/CASE DATA

Originating Agency Code (ORI)

Name of Validator (VLN)

RECORD IDENTIFYING DATA

ID Number (IDX)

Agency Case Number (OCA)

MODIFY AGENCY/CASE DATA

Originating Agency Code (ORI) Message Key (MKE)

Agency Case Number (OCA) Notify Originating Agency (NOA)

Date of Theft (DOT)

Linkage Agency Identifier (LKI) Linkage Case Number (LKA)

MODIFY GUN DATA

Serial Number (SER) Caliber (CAL)

Gun Make (MAK) Type (TYP)

Model (MOD)

Command:

FOX-PRIM T SPHQ00X8 TTESTER LOG 0 Message 10:29

Datamaxx Leading Law Enforcement Technology

4. While validating a record, modifications can be made to the record within the same transaction.
5. While validating, clearing or canceling a record within the file, the number of records to be validated with the file will decrease.
Example: If you validate one (1) of the twenty (20) records, the total number of records remaining to be validated will decrease to nineteen (19).

Operator's Lesson Plan

F. Automated Purges and Notification

1. Those records due for validation that are not updated by 2359 hours on last the day of the month will be automatically purged from IDACS/NCIC. An automated purge notice will be sent to the entering ORI.
2. The terminal agency should notify the non-terminal agency of any non-validated record purges.
3. Annual purges occur in January for records that reach their retention period. Guns, Unidentified, Missing and Wanted Persons remain in file until the entering agency removes the record. A missing person's record will be purged when a single locate is placed on the record.
4. Records that have been located are purged when the retention period is reached.
5. Protection Orders are purged on the expiration date, unless the expiration date is changed.

V. User ID Requests

1. Requests for User ID's should include a letter on department letterhead, a completed fingerprint card for each operator, a challenge question and answer for each operator and indicate if the operator is IDACS certified at another agency. The request must include the following:
 - a. Name to include any aliases and maiden names.
 - b. Date of Birth.
 - c. Social Security Number.
 - d. Results of III, CHRI, & Wanted File inquires (RF= Record Found, NR= No Record).
 - e. Level of certification the operator will need to be assigned (Full, Inq, MDD).
 - f. If operator is employed at more than one agency & also any past IDACS access operator has EVER held.
 - g. If your agency has a system that interfaces with the IDACS switch (such as MDD & CAD systems) you must include the User ID/LOGON assigned to your switch.
2. IDACS will assign ALL other User ID's.
3. Once IDACS has assigned a User ID it cannot be changed. Marriages, divorces or any other legal name change will not affect or change the User ID.

Operator's Lesson Plan

4. Challenge questions must be submitted along with the fingerprint cards and request for a User ID. Challenge questions should be a personal question that only the operator can answer. The challenge question and answer must be in a separate sealed envelop enclosed with the above. If the challenge question is not properly completed, the request will be returned to the agency to be corrected.
5. A User ID may be requested to be disabled by a switched message to IDACS (INISP0007) or a letter requesting the User ID be disabled. The request must indicate if the user is IDACS certified at another agency.

VI. Operator Background Policy and Procedures

1. In accordance with 240IAC 5-2-10, user agencies are required to guarantee the security clearance of all terminal and computer operators, including the submission of fingerprint cards to allow their background to be investigated.
2. The agency will assume full responsibility for all criminal history and wanted background checks for their agencies proposed IDACS operators. It is not the responsibility of the IDACS section to perform the checks or to obtain court documents and final dispositions.
3. All terminal agencies must complete the following when requesting a User ID:
 - a. Conduct a background check including but not limited to:
 1. Local criminal history check
 2. State criminal history check
 3. III criminal history check
 4. Inquire upon the following:
 - a. Maiden names.
 - b. Any name previously held
 - c. Alias names.
 - d. Additional DOB's or SSN's discovered in the background check.
4. When a record is discovered on a proposed operator a copy of the final disposition must be included with the proposed operator's information. The disposition will be reviewed and either approved or denied access by the Chairman of the IDACS Committee.
5. Forward along with the fingerprint card any criminal history records with disposition that is discovered.

Operator's Lesson Plan

6. Fingerprint Card Processing:
 - a. The card must be properly filled out with all applicable descriptive data. If the fingerprint card is not properly filled out, the entire request will be returned to the agency to be corrected.
 - b. The ORI block must show "INISP0000 CTR REC & ID-SPOL INDIANAPOLIS. IN."
 - c. The OCA block must contain the last seven (7) characters of your ORI ending with "IDX" (ex: 0520100IDX).
 - d. The "EMPLOYER" block must show the complete name and address of the requesting agency.
 - e. The reason fingerprinted block must contain: **"LAW ENFORCEMENT APPLICANT RE: IDACS/NCIC."**
 - f. Directions on the back of the card must be followed to insure good clear fingerprints.
 - g. Once the card is processed by ISP Records and the FBI, and no criminal record is found, a letter from the FBI with the heading "Civil Applicant Response" will be sent to the submitting agency for filing and must be available for inspection by the IDACS Security Officer. FBI fingerprint cards will no longer be returned to the submitting agency, unless there is a criminal record or the fingerprints are deemed unclassifiable. Fingerprints deemed unclassifiable will be returned to the agency to be reprinted.

If a copy of the fingerprint card is desired, the copy should be made by the agency prior to submitting to SP IDACS.
 - h. If the ISP or FBI records check reveals a criminal history record, the fingerprint card will be returned to IDACS, who will forward the card to the submitting agency for disposition.
 - i. All criminal history record information will be forwarded to the IDACS Section for review. Once reviewed by the IDACS Committee Chairman, a determination will be made as to whether or not the person will be permitted to be an IDACS operator.
8. Regional Computer Center Agencies/Agencies Accessing IDACS via a Computer Center including agencies with Mobile Data Devices (MDDs).

Operator's Lesson Plan

- a. The agency designated by the IDACS Committee as the Management Control Agency, will have the overall responsibility for the submission of the FBI applicant fingerprint card on all personnel connected with the Computer Center, i.e. data processing personnel as well as operators, and for agencies they service (this includes MDD agencies). Agencies served by the Center must submit a complete and accurate FBI applicant fingerprint card on each terminal operator to the Management Control Agency direct. Management Control Agencies of Computer Centers are given the option of retaining "Civil Applicant Response" for agencies that they service or returning those responses to the agency to be maintained.
- b. Processing of cards by the Management Control Agency will include checking their local files, and the forwarding them to the State Police IDACS Section.
- c. Any criminal record found must be brought to the attention of the IDACS Security Officer as soon as possible for further processing.
- d. The Management Control Agency will be responsible for the assignment of User ID's to all operators of agencies served by the Computer Center.
- e. Management Control Agencies will also be responsible for submitting to IDACS an alphabetical list of all persons fingerprinted by the 10th day of the even numbered months. This list must contain the NAME, User ID, and CERTIFICATION DUE DATE listing month, day, and year and be arranged according to agency.

VII. Quality Control

1. The following is information concerning quality control rules as listed in the Indiana Administrative Code (IAC).

240 IAC 5-1-1 General policy; restrictions on use

Authority: IC 10-1-1-3; IC 10-1-2.5-7

Affected: IC 10-1-2.5-2

- Sec. 1. (b) Accuracy is essential as is promptness in entering, modifying, locating, or clearing records in the system. Each record on file is identified with the agency originating that record and that agency alone is responsible for the accuracy, completeness, and correct status of that record at all times. IDACS cannot assume responsibility for the accuracy of any records entered by any agency.

Operator's Lesson Plan

2. IDACS/NCIC records must be kept accurate and up-to-date. Agencies that enter records in IDACS/NCIC are responsible for their accuracy, timeliness, and completeness. Stringent administrative procedures and controls to ensure that accurate data is entered in computerized criminal justice information systems are important. An officer's evaluation of information contained in a hit response is just as important as keeping the information accurate, timely, and complete. Combining stringent administrative controls with proper evaluation by the officer receiving the hit will prevent lost court cases, civil liability suits, and criminal charges against the law enforcement officer.
3. A second person must check the accuracy of IDACS/NCIC records. Verification should include assuring that all available information for entry was made e.g., VIN/License numbers, and that data in the IDACS/NCIC record matches the data in the investigative report. Agencies lacking support staff for this cross checking should require the case officer to check the record as he/she carries primary responsibility for seeking the fugitive and the stolen property.
4. Coordinators are to insure that all records entered for their agencies are checked for timeliness, completeness, and accuracy.
5. When notified by IDACS Quality Control that a record contains an error or has been cancelled because of a serious error, the Coordinator is to insure that the record is corrected or re-entered with the correct data as soon as possible.
 - a. An NCIC Administrative \$.E message indicates that NCIC has cancelled a record due to serious error, i.e., a wanted person record has been left in file after a locate has been placed against the record indicating the subject would not be extradited. If NCIC detects a serious error and cancels the record, IDACS will also cancel the record and notify the agency.
 - b. It is the responsibility of the Coordinator to insure that all terminal operators are aware of quality control procedures.
6. Ten Minute Hit Procedures
 - a. Upon receipt of an urgent hit confirmation request from an inquiring agency, the originating agency (ORI) of the record must within ten (10) minutes, furnish a substantive response, i.e., a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject the record.
 - b. Upon receipt of a routine hit confirmation request, the originating agency (ORI) of record has up to one (1) hour to reply to the request.

Operator's Lesson Plan

- c. It is the responsibility of the Coordinator to insure that all terminal operators utilize the Hit Confirmation Request and Response screen formats and follow the ten-minute hit procedures shown in the IDACS Manual.

VIII. Responsibilities to Non-Terminal Agencies Serviced

- 1. Coordinators are to assist non-terminal agencies in their area that they service with any IDACS related issues.
 - a. Questions on validations.
 - b. Questions on security of IDACS/NCIC/NELTS data.
 - c. Keeping agencies informed of all available data through IDACS/NCIC/NELTS.
 - d. Informing new agency head of IDACS.

IX. Where to Call for Assistance

- 1. SP IDACS Section
 - a. During normal business hours
 - 1. Format questions and or problems.
 - 2. Operational or administrative questions.
- 2. SP Data Operations Center (DOC)
 - a. Equipment Problems
 - 1. Due to the wide range of terminal equipment now being used, IDACS or SP Data Operations Center **will not** be able to assist with equipment problems.
 - 2. Prior to calling your vendor for service, check with Data Operations to determine if your terminal is acquired.
 - 3. Contact your vendor for any hardware problems.
 - b. After Normal Business Hours

Operator's Lesson Plan

1. Operational or format questions.
 2. Assist with expired passwords
 3. IDACS Chairman or Area Representatives
 - a. Can be contacted concerning any questions on IDACS/NCIC/NLETS policies and procedures.
 4. Regional Computer Centers
 - a. Agencies behind a regional computer center should contact the Regional Center Coordinator for any operational or equipment questions.
- X. IDACS Operator and Coordinator Certification Program
1. The following are training requirements as listed in the Indiana State Police Administrative Code (IAC).
- 240 IAC 5-2-11 IDACS Operator/Coordinator Certification Training**
- Authority: IC 10-1-1-3; IC 10-1-2.5-7**
Affected: IC 10-1-2.5-2
- Sec. 11. (a) All IDACS terminal operators (including mobile terminals) shall be trained and tested for their proficiency at operating the IDACS terminal. All IDACS coordinators shall be trained and tested for their proficiency at operating the IDACS terminal and for their skills as the coordinator.
2. The objectives of training requirements shall be as follows:
 - a. To insure that coordinators and terminal operators are familiar with the laws governing IDACS/NCIC/NLETS, IDACS system rules, regulations, and procedures, and what files and functions are available and how to utilize them properly.
 - b. Create an awareness of IDACS/NCIC/NLETS System capabilities in order to allow criminal justice agencies to obtain maximum use of the system.
 3. All persons assigned a User ID to operate the IDACS terminal and persons designated IDACS Coordinator by their agency shall be trained and tested according to the guidelines set forth by the IDACS Committee and approved by the State Police Superintendent.

Operator's Lesson Plan

4. Training course content is derived from the IDACS/NCIC/NLETS manuals and publications and will be periodically reviewed for relevancy, accuracy and updated accordingly.
5. The IDACS Committee can authorize the removal of a User ID, or impose sanctions on an agency for non-compliance with these procedures.
6. New terminal operators issued a User ID must be certified within the first six (6) months and re-certified every two years thereafter.
 - a. Coordinators must follow certification policies and regulations for scheduling operator's for schools and test-outs.
 - b. Coordinators must be certified as an operator and within the first six (6) months of appointment be certified as Coordinator, re-certified every two years thereafter.
7. Requests for class attendance must be submitted in writing from the agency head to the IDACS Section.
 - a. Any changes or cancellations in attendance must be in writing and received prior to the first day of class.

XI. IDACS User Agency Audits

1. IDACS User Agencies are periodically audited for compliance with rules, policies, and procedures.
 - a. Audits are conducted once every two years.
2. IDACS Audit Manual
 - a. Explanation in detail of what is reviewed during an audit.

XII. IDACS User Agency Sanctions

1. The following are sanction rules as listed in the Indiana Administrative Code (IAC). The IDACS sanctions policy is explained in Part 1 of the IDACS Manual.

240 IAC 5-2-12 User Agency Sanctions

Authority: IC 10-1-1-3; IC 10-1-2.5-7

Affected: IC 10-1-2.5-2

Operator's Lesson Plan

- Sec. 12. (a) The IDACS Committee shall review violations of IDACS rules and make recommendations to the State Police Superintendent to impose sanctions on user agencies.
2. The objectives of the sanction procedure shall be as follows:
 - a. To insure the integrity of the System
 - b. Create an awareness among user agencies of the importance of following rules, regulations, and procedures in order to minimize the risk to liabilities that may be incurred by misuse of the SYSTEM and its data.
 3. Sanctions shall be based upon the class of violation, any previous violations, and any exposure to criminal and civil liabilities that the violation might place on the SYSTEM, its officials, and the offending agency.
 4. Violations shall be classed as either Administrative (minor) or Security (serious) Violations. Security Violations are defined as one which has or could result in access of SYSTEM data by unauthorized individuals. All other violations are classed as Administrative.
 5. In determining the severity of the Violation, the type, Administrative or Security, and if any previous sanctions issued, shall be considered. The IDACS Committee may impose sanctions by one of the following:
 - a. Verbal Warning
 - b. Written Warning
 - c. Written Notice of Violation
 - d. Written Notice of Probation
 - e. Written Notice of Temporary Suspension
 - f. Written Notice of Permanent Suspension
 6. Temporary or permanent suspension of service will not begin, unless an emergency exists, until fifteen (15) days after the Agency Head has received written notice by certified mail or personal service.
 7. An Agency may apply to be reinstated if placed on permanent suspension on or after (1) year.

Operator's Lesson Plan

8. The IDACS Committee shall review violations of IDACS rules and make recommendations to the State Police Superintendent to impose sanctions on user agencies.
9. The IDACS Committee may impose sanctions in accordance with item (e) above.
10. The definition of Suspension means: A definite time period for the termination of direct access to the IDACS system data as imposed by the IDACS Committee.
11. Upon receiving a written notice of violation(s), the user agency head shall submit in writing to the Chairman of the IDACS Committee any disciplinary action taken and/or procedures to correct the violation. This reply shall be within 30 days of the receipt of the notice of violation.
12. The user agency or IDACS Committee agency may cancel the user agency agreement with 30 days notice.